Merchant Services– What You Need to Know

Heather Nowak – VP, CPP
Senior Product Manager

Agenda

- Overview of Merchant Services
  - Why accept cards?
  - What you need to know/consider
    - Capabilities/Pricing/Contract
    - Hardware/Software
    - Ongoing Support
- EMV, Tokenization/Encryption, and PCI (Oh My!)
  - What's the difference?
  - PCI - Let's take a closer look

Overview of Merchant Services

Why Accept Cards?

- 83% of consumers prefer to pay via card (credit card or debit card)
- Customer convenience
- Security for entity (no cash handling)
- Increases cash flow timeframe for merchant/business
- Multiple ways to accept cards (terminal, tablet, phone, website)

What You Need to Know/Consider:

- ***Capabilities***
  - Is integration needed with internal systems? Reporting Requirements?
  - Card only solution or other capabilities needed (check, ACH)
- ***Pricing***
  - Various pricing models exist – will depend on your card volume, types of cards accepted, average ticket
  - Other Fees:
    - Association Fees (MasterCard/Visa)
    - Tokenization/Encryption costs
    - Non PCI- Compliant
- ***Ongoing Support***
  - Understand the support model and ensure it aligns with your expectations
    - Sales representative? Call Center? Relationship Manager?
    - Hardware/Gateway support

EMV, Tokenization/Encryption, and PCI (Oh My!)

What’s the Difference?

- ***EMV***
  - Fraud liability shift to all point-of-sale devices (except Automated Fuel Dispensers) took effect October 2016
  - Liability for counterfeit fraud transactions shifts to merchant if cardholder presents and EMV capable card but the merchant does not have the technology to accept the EMV card
- ***Tokenization/Encryption***
  - Tokenization protects cardholder data after authorization so it can only be used on the processors network (changes card information into random digits – worthless to hacker)
  - Encryption protects cardholder data from point of swipe, at a terminal, until it reaches the processors network for authorization (end to end encryption)

- ***PCI (Payment Card Industry – Data Security Standard)***
  - https://www.pcisecuritystandards.org
  - Certification required by Associations (MasterCard/Visa)
    - Questionnaire completion and scans of websites
    - Submission of certification
    - Annual process

PCI – A Few Fun Facts

Only 29% of companies are compliant a year after validation

The average total cost of a data breach is $4 Million

PCI DSS compliance has increased by 167% since 2012

80% of organizations are still not compliant

You could pay $100,000 a month for being non-compliant…or much more

69% of consumers would be less inclined to do business with a breached organization

PCI – Let’s Take a Closer Look

PCI Data Security Requirements (applicable to anyone who accepts or processes cards)

- Build and Maintain a strong network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI – Let’s Take a Closer Look

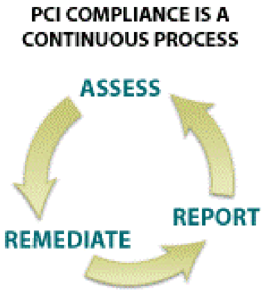
How to protect your business:

- Buy and use only approved PIN entry devices at your points-of-sale.
- Buy and use only validated payment software at your POS or website shopping cart.
- Do not store *any* sensitive cardholder data in computers or on paper.
- Use a firewall on your network and PCs.
- Make sure your wireless router is password-protected and uses encryption.
- Use strong passwords. Be sure to change default passwords on hardware and software – most are unsafe.
- Regularly check PIN entry devices and PCs to make sure no one has installed rogue software or “skimming” devices.
- Teach your employees about security and protecting cardholder data.

* - https://www.pcisecuritystandards.org/pci_security

PCI – Let's Take a Closer Look

The PCI 3-Step Process*



- ***Assess.***
  Identifying cardholder data, taking an inventory of IT assets and business processes for payment card processing, and analyzing them for vulnerabilities.
- ***Remediate.***
  Fixing vulnerabilities and eliminating the storage of cardholder data unless absolutely necessary.
- ***Report.***
  Compiling and submitting required reports to the appropriate acquiring bank and card brands.

* - https://www.pcisecuritystandards.org/pci_security/how

Contact Information:

Heather Nowak
Phone: 419-720-7708
Email: Heather.Nowak@Huntington.com